アクセス ログで、Windows 7/Vista クライアントからのトラフィックにユーザではなくワークステーションが表示されているのはなぜですか。

目次

質問

アクセス ログで、Windows 7 / Vista クライアントからのトラフィックにユーザではなくワークステーションが示されているのはなぜですか。

環境

Microsoft Windows 7、Microsoft Windows Vista、Cisco Web Security Appliance（すべてのバージョン）、サロゲート タイプ： IP アドレス

症状

アクセス ログの特定のログ行には、DOMAIN\USER の代わりにコンピュータのマシン名が示されます。

Microsoft は、「ネットワーク接続状態インジケーター」（NCSI）と呼ばれる新しい機能を Windows 7 と Windows Vista に導入しました。この機能は、システム トレイ内のネットワーク インターフェイス アイコンの上に表示される小さな地球アイコンとして示されます。 ログイン直後に、この機能がインターネットにデータを要求してインターネット接続が存在するかどうかを確認します。

NCSI には、NTLM 認証が必要な場合にユーザ クレデンシャルの代わりにマシン クレデンシャルが送信されるという既知の問題があります。

NCSI は、ほとんどの場合、最初の要求を PC から WSA に送信するため、サロゲートはまだ存在せず、実際のユーザ名の代わりにマシン名で新しい IP ベースのサロゲートが作成されます。 このサロゲートは、それがタイムアウトして、ユーザを実際のクレデンシャルで再認証しなければならなくなるまで、初期 IP アドレスからのすべての要求に使用されます。

このマシン名はほとんどの場合、最初に意図した AD グループのメンバーではないため、すべての要求が正しいアクセス/復号化ポリシーをトリガーせず、要求がブロックされることがあります。

NCSI に関する詳細については、次の Microsoft KB の記事を参照してください。

問題を回避するには、次の手順を参照してください。

1. タスク メニューで "regedit" を探してレジストリ エディタを起動します。 右クリックして、[Run as Administrator] を選択する必要があります。

2. 次のとおりに移動します。
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet

3. Internet キーの下で、[EnableActiveProbing] をダブルクリックしてから、Value データに「0」と入力します。
4. [OK] をクリックします。

5. コンピュータを再起動します。

これらの変更は、ドメイン コントローラを使用してグローバル ポリシー オブジェクト（GPO）としてすべてのクライアントにプッシュできます。

WSA での回避方法

NCSI の ID を作成し、URL またはそのユーザ エージェントに基づいてその認証を免除します。

NCSI が接続する既知の URL

ncsi.glbdns.microsoft.com
newncsi.glbdns.microsoft.com
www.msftncsi.com

NCSI ユーザ エージェント

Microsoft NCSI